1. What is SSRF?

What is SSRF (Server-Side Request Forgery)?

At its core, **SSRF (Server-Side Request Forgery)** is a vulnerability where an attacker can make a target server send unauthorized requests to other systems. These requests are controlled by the attacker, and the server acts as their puppet to access resources it shouldn't.

Breaking it Down:

1. **Server Makes Requests on Your Behalf:**
   In many web applications, servers make HTTP requests to fetch external resources, like images, APIs, or files. SSRF abuses this functionality.
2. **Attacker Controls the Request:**
   If an attacker can influence the **URL** or **target of the request**, they can direct the server to:
   - Fetch sensitive information from private/internal systems.
   - Perform actions the attacker can't do directly.

A Simple Analogy:

Imagine a secure house (the server). Only the owner (you) is allowed inside, but you have a butler (the server) who takes requests from anyone standing at the gate.

- The attacker (a stranger) tells the butler:
  "Please fetch the secret documents from the vault."
- The butler doesn’t know better and retrieves the sensitive data for the attacker. 💥

Key Features of SSRF:

- **Uses the server as a proxy** to access other systems or resources.
- Targets both **internal resources** (e.g., localhost, private network) and **external APIs** (cloud services, public APIs).
- Can lead to serious breaches, including exposing **metadata, credentials**, and performing **privilege escalation.**
